ABSTRACT

An efficient implementation of zero knowledge protocols for authentication of devices and for identification of devices connecting to a network. According to one aspect, the present invention provides a method of verifying the knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.